PRIVACY INTERNATIONAL

Submission for the 2013 United Nations Forum on Business and Human Rights

This is a submission by Privacy International (PI), a London-based human rights organisation that works to advance the right to privacy and fight surveillance around the world. PI wishes to propose as a topic for the 2013 Forum of Business and Human Rights **the international trade in surveillance technologies**, with a particular focus on the responsibilities of Western business enterprises producing and exporting surveillance technology that is used by repressive regimes around the world, and the responsibility of States to enact adequate export controls to regulate these technologies.

Potential speakers: Eric King (Privacy International), Cynthia Wong (Human Rights Watch), Christopher Soghoian (American Civil Liberties Union), Ben Wagner (European University Institute), Susan Morgan (Global Network Initiative)

Contact point: Eric King
Head of Research, Privacy International
Tel.: +44 (0) 20 7242 2836
Email: eric@privacy.org

Surveillance technology and the UN "Protect, Respect and Remedy" Framework

The international trade in surveillance technology is a pertinent topic for the 2013 Forum on Business and Human Rights, engaging the Forum's Guiding Principles on Business and Human Rights and the "Protect, Respect and Remedy" framework on many points.

Regarding the **State's duty to protect (Pillar I)** against human rights abuse by third parties, there has been a manifest failure on the part of Western governments to take appropriate steps by tightening export controls on surveillance technology. This is exemplified by the UK government's unsatisfactory response to PI's efforts to engage them on the issue of introducing stronger export controls on surveillance technology, and its possible failure to enforce licensing requirements on technologies that are currently listed (see below). In accordance with Guiding

Principle **B3(a)**, States should be encouraged to adopt tighter export controls which will stop technology companies aiding and abetting repressive regimes in their human rights abuses.[1] It is also crucial that governments enforce any export controls already in place, ensuring that companies obtain licences to export products where this is required.

In accordance with Guiding Principle **B3(c)**, States should also be encouraged to provide effective guidance to technology companies on how to respect human rights throughout their operations, including guidance on the adoption of human rights due diligence and human rights policies. States should exert pressure on companies to uphold a policy whereby they do not export mass surveillance equipment to countries which have a poor human rights record and where it is likely that such equipment will be used for unlawful purposes.

In relation to States that buy surveillance technology, those States should, in accordance with Guiding Principle **B6**, ensure that the companies with whom they are contracting uphold human rights, by having in place human rights due diligence and a human rights policy.

According to the Guiding Principles, it is also the duty of States and governments to review the effectiveness of their legislation and policies. Given that there has been a failure on both the national and international levels to effectively control the trade in surveillance technology, reviews of both national and international export control regimes are urgently needed. On the international level (and in accordance with Guiding Principle **B10**), States should co-operate in ongoing negotiations and amendments to the Wassenaar Arrangement, which in its current form does not sufficiently regulate the export of surveillance technology, with the result that lists of restricted products and countries are regularly updated and ideally that the export of all mass surveillance technology and equipment is restricted. Individually, States should aim to implement the Wassenaar Arrangement expansively, adding to its provisions such that export of surveillance technology is effectively controlled.

Regarding the duty of States in conflict-affected areas (Guiding Principle **B7**), the ban by the EU and the United States on the export of surveillance technology to Syria and Iran is an example of positive action and initiative taken by States to help ensure that companies are prevented from contributing to human rights abuses where they are most likely to occur. The willingness shown

[1] See below for explanation and evidence concerning the way in which Western-manufactured surveillance technology has contributed towards repression and human rights abuse in repressive regimes.

by States to impose export controls on surveillance technology in the cases of Syria and Iran should be extended and applied in the case of other repressive regimes, where the likelihood of human rights abuses occurring is as strong as that in conflict-affected areas.

Regarding the **corporate responsibility to respect (Pillar II)**, the lack of respect or concern for human rights by many companies that sell surveillance technologies is of concern. Whilst the strongest onus should be on the State to promote companies' (as well as citizens') respect for human rights and awareness of the human rights consequences associated with surveillance technology, by implementing appropriate legislation and policies as well as instigating dialogue, the companies themselves should be encouraged to avoid contributing to human rights abuses and to address adverse human rights impacts where they do occur. To this end, and in accordance with Guiding Principles **B15 and B17**, companies should universally integrate effective human rights due diligence into their operations: such due diligence would involve undertaking comprehensive research into potential government clients, including their domestic laws and practices regarding privacy, communications and surveillance, and their treatment of political dissidents, human rights defenders, activists, journalists, lawyers and ethnic/religious minorities (who are most commonly the targets of unlawful surveillance). Companies should also ensure that they continuously and regularly monitor the use of their products, and have processes in place that enable remediation of rights abuses and deactivation of the relevant products. Companies should also implement a comprehensive human rights policy which contains an undertaking not to export surveillance products to countries which have a poor human rights record and where it is likely that the company's surveillance products will be used for unlawful purposes, such as repressing political dissidents and human rights activists.

In addition, Guiding Principles B16, B18, B19, B20, B21, B22 and B23, all of which concern businesses' engaging with and mitigating the negative human rights impact of their activities, are particularly relevant and applicable in the case of companies that supply surveillance technology and equipment.

Regarding **access to remedy (Pillar III)**, victims of human rights abuses associated with surveillance technology are often the citizens of repressive regimes and are generally subjected to those abuses at the hands of the government or law enforcement agencies (whose actions are mandated by the government) that operate under the repressive regime. It cannot be expected that such victims should seek or be provided with redress from the very State that perpetrated the human rights abuses. Thus there is a duty on States and companies that supply

surveillance technology to work out adequate grievance mechanisms and punitive sanctions for those affected and concerned. Where a company has acted in breach of the law by exporting surveillance technology without having obtained a licence (if it is required to do so), the State should have in place adequate punitive sanctions, such as fines. Of course, if the surveillance technology in question is not regulated and the company has not acted unlawfully in exporting surveillance equipment, the ability of the State to provide redress to victims whose rights have infringed by abuse of the technology is limited.

At this point, there should be adequate access to remedy provided by international, non-judicial mechanisms such as the Organisation for Economic Co-operation and Development (OECD) and the State-level National Contact Points (NCPs). Currently, however, the remedial response of the OECD and NCPs is limited to publishing a concluding statement on the outcome of their investigation into breaches committed by the offending company. Thus, whilst the process can result in damage to a company's reputation and goodwill, it cannot provide victims with substantial and adequate redress.

Additionally, operational-level grievance mechanisms administered by companies themselves (in accordance with Guiding Principle **B28**) should be encouraged as a way of providing victims with access to remedy. As suggested in the Guiding Principles, such a mechanism has certain benefits such as speed of access and remediation, and reduced costs. In the case of companies that supply and maintain surveillance technology for use by third parties, they are in a position to know early on whether and where such equipment is being abused. However, the effectiveness of such a grievance mechanism depends on a business' impartiality, integrity and ability to accord due process. Such mechanisms need to be supported and promoted by the State.

International Trade in Surveillance Technologies

Since 2011 PI has been running a project entitled Big Brother Incorporated, a global investigation into the international trade in surveillance technologies, which is worth an estimated $5 billion a year. Surveillance technologies can be defined as technologies which can monitor, track and

assess the movements, activities and communications of individuals. The capabilities of such technologies have grown hugely in the past decade, and include an array of visual recording devices, bugging equipment, computer information systems and identification systems; surveillance technology ranges from malware which infects a target computer to record every keystroke, to systems for tapping undersea fibre-optic cables in order to monitor the communications of entire populations. These innovations are used by military, police and intelligence authorities as technologies of repression: in various repressive regimes around the world, these technologies have become instrumental in perpetrating human rights abuses against political activists, dissidents and citizens in general, including violation of their right to privacy and free speech, torture, arbitrary arrest and even extra-judicial killings.

PI regards the enactment of strict export controls by all States that export surveillance technologies as urgently needed. PI's main objectives are: i) to raise worldwide awareness of the dangers of surveillance technologies and the ethical failures of the surveillance industry; ii) to ensure that export controls are put in place in Europe and the US to restrict the sale of surveillance technologies to repressive regimes; and iii) to seek redress for those who have suffered harm as a result of Western-manufactured surveillance technologies.

There is growing international momentum towards stricter regulation of surveillance exports. In the past year, the EU Parliament passed a resolution calling for stricter oversight of surveillance technology exports[2], President Obama announced an executive order to prevent such exports to Syria and Iran[3], and the French Secretary of State for the Digital Economy signaled a sea change in France's export policies[4]. In addition, it was announced in the Public Statement of the 2012 Plenary Meeting of the Wassenaar Arrangement that export controls had been strengthened in the area of passive counter-surveillance equipment of mobile telecommunications.[5]

---

[2] European Parliament News, 'Controlling dual-use exports', 27th September 2011, available at: http://www.europarl.europa.eu/news/en/pressroom/content/20110927IPR27586/html/Controlling-dual-use-exports

[3]The White House Blog, 'Fact Sheet: A Comprehensive Strategy and New Tools to Prevent and Respond to Atrocities', 23rd April 2012, available at: http://www.whitehouse.gov/the-press-office/2012/04/23/fact-sheet-comprehensive-strategy-and-new-tools-prevent-and-respond-atro

[4] Epelboin, F., Reflets, 'Is France about to End Exporting Surveillance Technology?', 24th July 2012, available at: http://reflets.info/is-france-about-to-end-exporting-surveillance-technology/

[5]http://www.wassenaar.org/publicdocuments/2012/WA%20Plenary%20Public%20Statement%202012.pdf

PI is currently engaged in research and investigation, public campaigning, political engagement and strategic litigation aimed at bringing to light the abuses of the surveillance industry and ensuring that it is properly regulated in future.

Last year PI commenced legal action against the UK government[6] for its failure to control export of surveillance technologies; we wrote a letter to the Secretary of State for Business, Innovation and Skills (BIS) asking why the government had failed to take any concrete steps to stop British surveillance technology being exported to regimes that routinely engage in internal repression and serious human rights breaches including unlawful detention, torture and enforced disappearance. In its response, the Secretary of State did not reassure us that it intended to extend the existing regime to include comprehensive and effective oversight of all surveillance technology exports, though it revealed that the department had conducted an assessment of FinSpy (a suite of surveillance products sold by the UK-based firm Gamma International, which PI cited in its original letter as an example of a particularly dangerous piece of surveillance technology), and concluded that such products fell within the purview of the existing export control regime. In a subsequent letter, BIS admitted that Gamma International had yet to apply for, or be granted, any such licence. Despite this, FinSpy and similar products have turned up in Australia, Bahrain, Bangladesh, Brunei, Canada, Czech Republic, Estonia, Ethiopia, Germany, India, Indonesia, Japan, Latvia, Malaysia, Mexico, Mongolia, Netherlands, Qatar, Serbia, Singapore, Turkmenistan, United Arab Emirates, the United States, and Vietnam. PI subsequently wrote to HM Revenue & Customs (the department responsible for enforcing export controls), enclosing a 186-page dossier of evidence, alerting the department to this ongoing breach of UK export regulations. After no response was forthcoming, PI sent a follow up letter in December 2012, stating that HMRC should be following the Victim's Code of Practice. HMRC subsequently responded, stating that they were statutorily barred under s17 of the Freedom of Information Act 2000 from disclosing information about their primary purpose. PI subsequently tried and failed to contact HMRC by telephone, and finally sent a pre-action protocol letter for judicial review. On 5th April 2013, PI filed a judicial review claim against HMRC.

In addition to trying to effect change on export controls at the State level, PI has also taken direct action against the businesses concerned themselves. In February 2013 PI and its partner organisations the European Center for Constitutional and Human Rights, Reporters Without

[6] Privacy International, available at: https://www.privacyinternational.org/press-releases/privacy-international-commences-legal-action-against-british-government-for-failure

Borders, Bahrain Center for Human Rights and Bahrain Watch filed OECD complaints[7] with the UK and German National Contact Points (NCPs) against Gamma International and Trovicor GmbH, companies who develop and supply surveillance technology, in connection with emerging evidence of abuse of their technologies by government authorities in Bahrain. The complaints addressed the ways in which the companies might have breached the OECD Guidelines for Multinational Enterprises by facilitating human rights abuses by authorities in Bahrain. It was alleged in the complaints that Gamma and Trovicor may have breached the human rights chapter of the Guidelines, by aiding and abetting the Bahraini authorities in their perpetration of various human rights abuses on Bahraini citizens. The complaints highlight how use of such surveillance equipment has the potential to bring about multiple human rights abuses, including unlawful violation of privacy, suppression of free speech, arbitrary arrest, torture and even extrajudicial killing. Evidence from security researchers at Citizen Lab, a laboratory based in the Munk School of Global Affairs at the University of Toronto that has been conducting expert analysis of the infected devices, was cited in the complaints. Citizen Lab had analysed the FinFisher-infected devices of three victims - Ala'a Shehabi, Husain Abdulla and Shehab Hashem – and their research demonstrates how the devices are targeted: Gamma's FinFisher products work by installing malicious software onto a user's computer or mobile phone without the user's knowledge, which is accomplished by tricking the user into downloading fake updates from what appear to be legitimate sources, such as BlackBerry, iTunes or Adobe Flash. Once the user accepts these updates, the computer or mobile phone is infected, enabling full access to the information held on it, including access to emails, social media messaging and Skype calls. Shehabi, Abdulla and Hashem were all sent emails with attachments on topics of interest to them (Shehabi and Hashem received exactly the same email). Citizen Lab's research also suggested that Gamma were continuing to update FinFisher software for use by the Bahraini authorities. Citizen Lab has published its findings in two expert reports, entitled 'From Bahrain with Love: FinFisher's Spy Kit exposed?'[8] (published on 9th July 2012) and 'The Smartphone Who Loved Me: FinFisher Goes Mobile?'[9] (published on 11th August 2012).

[7] Privacy International, available at: https://www.privacyinternational.org/press-releases/human-rights-organisations-file-formal-complaints-against-surveillance-firms-gamma
[8] The report can be found at: https://citizenlab.org/wp-content/uploads/2012/08/09-2012-frombahrainwithlove.pdf
[9] The report can be found at: https://citizenlab.org/wp-content/uploads/2012/08/11-2012-thesmartphonewholovedme.pdf

The complaints also examine the case of Abdul Ghani al-Khanjar, whose mobile phone was infected by Trovicor malware and who was subsequently detained in prison for six months in 2010 and tortured by Bahraini authorities.[10]

Since the complaints have been filed, Citizen Lab has released a further report, entitled 'You Only Click Twice: FinFisher's Global Proliferation'[11] uncovering evidence that Gamma International's FinFisher products are being used in 25 countries, including Australia, Bahrain, Bangladesh, Brunei, Canada, Czech Republic, Estonia, Ethiopia, Germany, India, Indonesia, Japan, Latvia, Malaysia, Mexico, Mongolia, Netherlands, Qatar, Serbia, Singapore, Turkmenistan, United Arab Emirates, United Kingdom, United States, and Vietnam.

Expert and media analysis has brought to light a number of other companies which have been mired in controversy due to evidence of their surveillance products being used by authorities of repressive regimes. Theses include Amesys[12] (a French company and an ex-subsidiary of Bull), VASTech Ltd[13] (a South African company), and ZTE Corporation[14] (a Chinese company), whose surveillance products, along with those supplied by Gamma and Trovicor, were found to be in use in government and law enforcement agencies of Mubarak's Egypt and Gaddafi's Libya in 2011, after those regimes were overthrown.

PI has identified 140 companies around the world that are known to be selling surveillance technologies. In March 2012 PI wrote to those companies asking them a series of questions aimed at ascertaining what due diligence they conduct when dealing with foreign companies or governments, how many of them were doing business or seeking to do business with 'Not Free' countries (as categorised by Freedom House's reports), and whether any of them would be

---

[10] Vernon Silver and Ben Elgin (Bloomberg News reporters) have reported on the case of Abdul Ghani; available at: http://www.bloomberg.com/news/2011-08-22/torture-in-bahrain-becomes-routine-with-help-from-nokia-siemens-networking.html

[11] The report can be found at: https://citizenlab.org/wp-content/uploads/2013/04/15-2013-youonlyclicktwice.pdf

[12] Gallagher, R., Slate, 'French Company that Sold Spy Tech to Libya Faces Judicial Inquiry Amid New Allegations', 19th June 2012, available at: http://www.slate.com/blogs/future_tense/2012/06/19/amesys_facing_inquiry_in_france_over_selling_eagle_surveillance_technology_to_qaddafi_.html; Owni, 'How Gaddafi Spied On the Fathers of the New Libya', available at: http://owni.eu/2011/12/01/exclusive-how-gaddafi-spied-on-the-fathers-of-the-new-libya/

[13] Sonne P. and Coker, M., Wall Street Journal, 'Firms Aided Libyan Spies', 30th August 2011, available at: http://online.wsj.com/article/SB10001424053111904199404576538721260166388.html

[14] *Ibid.*

interested in meeting with PI to discuss their human rights policies. It was notable that, of these 140 companies, 48 were American, 21 British and 12 German. In contrast, there were very few companies based in countries where use of surveillance technology has raised concerns. These statistics, together with evidence (outlined above) of Western surveillance products being found in many countries worldwide, overwhelmingly suggests that repressive regimes tend to buy equipment from US and European countries rather than manufacture it themselves. Thus any action taken by the US, UK and German governments (in particular) to control exports would be effective in limiting the kinds of advanced and sophisticated equipment that repressive regimes are able to use as a means of repressing citizens and committing human rights abuses.

On an international level, surveillance technologies are not sufficiently controlled by the Wassenaar Arrangement, the multilateral export control regime to which 41 countries have subscribed. Most surveillance technologies do not fall within the Wassenaar Arrangement's Munitions List or Dual-Use List, and many companies are able to avoid being caught under the Arrangement by marketing their products as intended for civilian or dual use (i.e. not specifically military use), despite the likelihood that their products are being subject to military end-use as well as for repressive purposes: thus, for example, VASTech Ltd was not required to obtain a licence from the South African government for exporting its mass telephone surveillance equipment to Libya, due to the fact that although the equipment can be categorized as "*electronic systems, designed…for surveillance and monitoring of the electro-magnetic spectrum"* in accordance with provision ML 11 a (c) (on the Munitions List), it cannot be definitively classed as "*specially designed for military use"* or "*for military intelligence or security purposes*", and thereby avoids falling under this provision.